METHOD AND APPARATUS FOR MANAGEMENT OF ENCRYPTED DATA THROUGH ROLE SEPARATION

ABSTRACT

One embodiment of the present invention provides a system for managing a database that stores sensitive information. Upon receiving a command to perform an administrative function involving an object defined within the database system, the system determines if the object is a sensitive object that is associated with security functions in the database system. If the object is not a sensitive object, and if the command is received from a normal database administrator, the system allows the administrative function to proceed. On the other hand, if the object is a sensitive object, and if the command is received from a normal system administrator, the system disallows the administrative function. In one embodiment of the present invention, the system additionally receives a request to perform an operation on a data item in the database system. If the data item is a sensitive data item containing sensitive information, and if the request is received from a sensitive user who is empowered to access sensitive data, the system allows the operation to proceed if the sensitive user has access rights to the data item. Otherwise, if the data item is a sensitive data item and the request is received from a normal user, the system disallows the operation. In one embodiment of the present invention, if the data item is a sensitive data item, if the operation is allowed to proceed, and if the operation involves retrieval of the data item, the system decrypts the data item using an encryption key after the data item is retrieved. In a variation on this embodiment, this encryption key is stored along with a table containing the data item. Note that this encryption key is preferably stored in encrypted form.